



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/240,265	01/29/1999	MARK E. PETERS	CR9-98-095	7166

25259 7590 10/09/2003

IBM CORPORATION  
3039 CORNWALLIS RD.  
DEPT. T81 / B503, PO BOX 12195  
REASEARCH TRIANGLE PARK, NC 27709

EXAMINER
----------

MEISLAHN, DOUGLAS J

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 10/09/2003

14

Please find below and/or attached an Office communication concerning this application or proceeding.

9

# Office Action Summary

Application No.

09/240,265

Applicant(s)

PETERS, MARK E.

Examiner

Douglas J. Meislahn

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 17 July 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-9 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-9 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

## Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 12.
- 4) ☐ Interview Summary (PTO-413) Paper No(s) \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## **DETAILED ACTION**

### ***Response to Amendment***

1. This action is in response to the amendment filed 17 July 2003 that amended claims 5 and 6 while adding claims 7-9.

### ***Response to Arguments***

2. Applicant's arguments filed 17 July 2003 have been fully considered but they are not persuasive.

3. Applicant partakes in a piecemeal analysis of the references, all the while generally remaining silent as to features of the present claims that are not shown by the cited prior art. The limitation that applicant does cite as being absent from the references is "extension", which applicant says is a term that has a known meaning within the art of X.509 certificates. While this is correct, the known meaning is not definite, as exhibited by Aucsmith et al.'s (6175626) and Sudia et al.'s (5995625) fifth figures, both of which show X.509 extensions. (Sudia et al.'s extension is made of elements 50 and 52.) Given the vagaries of what elements are necessarily part of an X.509 extension, the examiner has interpreted the word in its broadest, reasonable sense. As such, the bits in Shambroom that identify the cryptographic algorithms, which are additional information, read on an extension. The examiner recommends adding a clause to the independent claims that specifically lays out what applicant views as minimum requirements for an X.509 extension in the instant invention.

4. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections

are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

5. Applicant responds to the examiner's previous commentary on applicant's previous arguments. The first two paragraphs are discussed above. Applicant's third paragraph in this section returns to the subject of extension, which have been discussed above.

6. Applicant considers the motivation to combine *Shear et al.* with *Shambroom* to be less than compelling, partly because *Shear et al.* is not directed to certificates. The examiner is of the opinion that *Shear et al.*, while specifically directed to load modules, executables, and other data elements, teaches multiple signatures created with dissimilar algorithms in a broadly applicable fashion, and thus the combination is proper. Furthermore, digital certificates are data elements, and hence *Shear et al.* is directly applicable thereto.

7. Structure for data is not statutory. Creating or modifying the data according to the structure is statutory. Program means or an apparatus for performing the steps of creating or modifying the data according to the structure is statutory.

8. Applicant's arguments with respect to the applicability of the 101 rejection are unpersuasive because applicant's argument rests on mentioning claims in an unrelated case. Applicant is advised to cite case law showing that structure for data is patentable.

***Claim Rejections - 35 USC § 101***

9. 35 U.S.C. 101 reads as follows:

Art Unit: 2132

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10. Claims 1-3 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-3 claim data, which is nonfunctional descriptive material. As such, embodying the data on a computer-readable would NOT make the claims statutory. See MPEP 706.03(a) and, especially, 2106 IV B 1 (b).

***Claim Rejections - 35 USC § 103***

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. Claims 1-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shambroom (5923756) and Schneier (*Applied Cryptography*) in view of Shear et al. (6157721).

In lines 32-35 of column 10, Shambroom discusses a certificate that includes a public key and list of one or more cryptographic algorithms supported by the entity associated with the public key. The certificate can resemble an X.509 certificate. On pages 574 and 575, Schneier describes the X.509 certificate. As can be seen in figure 24.2, the certificate includes a section that identifies the algorithm, parameters, and a public key. There is also a section for a signature. These read on the first clause of applicant's first claim. The list of algorithms disclosed in Shambroom also anticipates an extension for identifying at least one alternative algorithm. Shambroom does not

dictate that a second public key and signature therefor be included in the certificate. In their abstract, Shear et al. say that using several dissimilar digital signature algorithms and their resultant signatures may "reduce the scope of any specific compromise." Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to put multiple signatures formed with different algorithms in Shambroom's exemplary X.509 certificate, thereby protecting the data from compromise. Inclusion of the secondary public key in the certificate would save an authenticator from tracking it down, thereby increasing efficiency.

With respect to claim 2, pages 480 and 481 of Schneier discuss elliptic curve public key systems. RSA is first mentioned on page 17. According to Schneier, it is the most popular public-key algorithm. There are trade-offs between the two, particularly in terms of the relative computational workloads of the two entities (signer and verifier). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to support RSA and an elliptic curve cryptosystem with the X.509 certificate taught by Shambroom.

Both signatures verify at least part of the certificate and hence read on claim 3. Claims 4-6 and 7-9 are largely the same as claims 1-3 and are rejected on the same grounds.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703)

①

Art Unit: 2132

305-1338. The examiner can normally be reached on between 9 AM and 6 PM,  
Monday through Thursday.

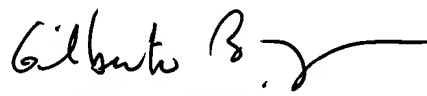
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.



DJM

Douglas J. Meislahn  
Examiner  
Art Unit 2132



GILBERTO BARRÓN  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100